

JUN 28 2023

1. From in or around July 2021 until in or around March 2023, in the Northern District of Ohio, Western Division, and elsewhere, Defendants EMMANUEL OKEREKE, OLABODE BANKOLE, INDIA BARNES, OLALEKAN BASHIRU, ARUAN DRAKE, EMMANUEL ESSILFIE, JEREMIAH GLINSEY, LON GOODMAN, D'ANDRE HASTY, KINGSLEY OWUSU, ANTON PARKER, and CARLTON PRUITT, together with others known and unknown to the Grand Jury, knowingly combined, conspired, confederated, and agreed with each other, and with others known and unknown to the Grand Jury, to commit an

offense under Title 18, United States Code, Chapter 63, to wit: knowingly devised, and intended to devise, a scheme and artifice to defraud and to obtain money and property by means of false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud and attempting to do so, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, and pictures, in violation of Title 18, United States Code, Section 1343.

2. The scheme generally worked as follows. Unknown co-conspirators, likely overseas, maintained a computer hacking campaign targeting individuals, businesses, and other organizations in the United States and elsewhere. The campaign's object was to gain access to genuine e-mail accounts held by individual users. The co-conspirators would then monitor the communications and other activities of the individual users in order to learn each user's business practices and contacts.

3. After gaining sufficient intelligence about the nature of the hacking victim's activities, the co-conspirators would send a fraudulent e-mail to either the hacking victim, or to someone communicating with the hacking victim, requesting payment. Because the co-conspirators were familiar with the victim's activities, the fraudulent e-mails could be crafted in a way to convince the recipient that the request for payment was genuine.

4. The fraudulent e-mails generally took three forms, each of which included false and fraudulent pretenses, representations, and promises:

a. *Spoof e-mails.* Having hacked a victim's e-mail account, the co-conspirators may have learned, for example, that the victim owed money to a creditor with whom the victim was in regular contact. After learning the nature of the debt, the co-conspirators would create an e-mail account with an address

closely resembling the creditor's address. The co-conspirators would then send a "spoof" e-mail from this new account to the hacking victim with payment instructions. Believing the "spoof" e-mail to be genuine, the victim would send the money as directed, not knowing that the funds were being deposited into a bank account controlled by someone conspiring with the sender of the "spoof" e-mail.

b. *E-mails to third parties from hacked accounts.* After hacking a victim's e-mail account, the co-conspirators may have learned that the victim was demanding payment from a debtor with whom the victim was in regular contact. Because the co-conspirators already controlled the genuine e-mail account, there was no need to create a new "spoof" e-mail account. Instead, the co-conspirators used their control of the hacked e-mail account to send an e-mail to the debtor demanding payment into a bank account controlled by another co-conspirator. The debtor would comply, not knowing that they were sending money to a bank account controlled by one of the conspirators and not to the individual actually owed the debt. Defendants similarly used this method to request account withdrawals, for example, by sending an e-mail to a victim's investment broker directing a withdrawal to be deposited in a co-conspirator's account.

c. *Internal e-mails from hacked accounts.* The computer-hacking co-conspirators hacked e-mail accounts belonging to corporate officers, such as a victim corporation's CEO. The conspirators would then send an e-mail from the CEO to the corporation's financial officer instructing him to make payment for a



given purpose. The financial officer would comply and send the funds to a bank account controlled by another conspirator.

5. Defendants here were in charge of maintaining an ample supply of domestic bank accounts into which their computer-hacking co-conspirators could direct victim payments.

Defendants did this using one, all, or a combination of the following methods:

a. *Synthetic Identities.* Defendants created numerous synthetic identities, which they used to open bank accounts. These identities were synthetic in that they did not belong to real people, but instead relied on a fabricated name, social security number, residential history, and similar information.

b. *Shell Companies.* Defendants would use both these synthetic identities and their own identities to pose as business owners seeking to open accounts in the names of shell companies that they created solely for the purpose of fraudulently legitimizing and concealing the receipt and disbursement of fraud proceeds.

c. *Personal Accounts.* On occasion, Defendants used accounts in their own names to receive and disburse fraud proceeds.

6. Defendants furthered the scheme to defraud by transmitting or causing to be transmitted e-mail communications and transferring or causing to be transferred funds, with both types of transmissions being sent by means of wire communication in interstate and foreign commerce. These wire communications were sent from, to, and through the Northern District of Ohio from places outside the Northern District of Ohio.

7. Defendants also furthered the scheme to defraud by concealing it. They did so by quickly disbursing the funds from the accounts into which they were deposited, thus frustrating

attempts to recover the funds if the fraud were discovered. Defendants disbursed these funds with cashier's checks payable to shell companies and others.

8. In all, the scheme defrauded at least 50 victims. Although some funds were frozen or recovered, the scheme nonetheless convinced victims to part with at least \$10,000,000. Those victims resided throughout the United States, including Ohio, New York, California, Texas, and Florida. Victims also resided in Canada, Mexico, Bermuda, and Romania.

9. It was part of the scheme that:

- a. OKEREKE and BASHIRU directed the conspiracy's activities in Chicago.
- b. BANKOLE and HASTY directed the conspiracy's activities in Atlanta.
- c. GOODMAN owned and operated New Dolton Currency Exchange.

GOODMAN allowed Defendants to cash fraudulent checks at the New Dolton Currency Exchange, and retained a portion of the proceeds for himself.

GOODMAN also sent emails to financial institutions in an effort to conceal the scheme.

- d. BASHIRU, DRAKE, GLINSEY, OKEREKE, and PARKER negotiated checks containing fraud proceeds.

- e. BARNES, ESSILFIE, GLINSEY, HASTY, OWUSU, PARKER, and PRUITT opened bank and related accounts using synthetic identities.

Acts in Furtherance of the Conspiracy

10. In furtherance of the above schemes, and to effect the objects and conceal the existence thereof, Defendants and others performed acts in the Northern District of Ohio and elsewhere, including, but not limited to, the following:

- a. On or about March 10, 2022, a co-conspirator caused Victim Business 1 of Chagrin Falls, Ohio, to transmit an interstate wire transfer of \$75,631.
- b. On or about April 15, 2022, a co-conspirator caused Victim Business 2 of Hudson, Ohio, to transmit an interstate wire transfer of \$20,000.
- c. On or about April 28, 2022, a co-conspirator caused the Huron County Emergency Management Agency in Norwalk, Ohio, to transmit an interstate wire transfer of \$165,693 to a bank account controlled by GLINSEY.
- d. On or about August 12, 2022, a co-conspirator caused Victim Business 3 of Hudson, Ohio, to transmit an interstate wire transfer of \$331,814.
- e. On or about November 21, 2022, a co-conspirator registered "DMG Food Co." with the Ohio Secretary of State's Office.
- f. On or about December 1, 2022, a co-conspirator opened a PNC Bank account in Independence, Ohio, in the name of DMG Food Co.
- g. On or about December 6, 2022, a co-conspirator caused Victim Business 4 of Hopkins, South Carolina, to transmit an interstate wire transfer of \$150,000 to the DMG Food Co. PNC Bank account registered in Independence, Ohio.

All in violation of Title 18, United States Code, Section 1349.

COUNT 2  
(Money Laundering Conspiracy, 18 U.S.C. § 1956(h))

The Grand Jury further charges:

- 11. The factual allegations of paragraphs 1 through 10 of this superseding indictment are incorporated herein by reference.
- 12. From in or around July 2021 until in or around March 2023, in the Northern District of Ohio, Western Division and elsewhere, Defendants EMMANUEL OKEREKE,



OLABODE BANKOLE, INDIA BARNES, OLALEKAN BASHIRU, ARUAN DRAKE, EMMANUEL ESSILFIE, JEREMIAH GLINSEY, LON GOODMAN, D'ANDRE HASTY, KINGSLEY OWUSU, ANTON PARKER, and CARLTON PRUITT, together with others known and unknown to the Grand Jury, knowingly and intentionally combined, conspired, and agreed with each other to commit offenses against the United States, in violation of Title 18, United States Code, Sections 1956 and 1957, to wit:

a. knowingly conducting and attempting to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of a specified unlawful activity, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of the specified unlawful activity and that while conducting and attempting to conduct such financial transaction knew that the property involved in the financial transaction represented the proceeds of some form of unlawful activity, in violation of Title 18, United State Code, Section 1956(a)(1)(B)(i), and

b. knowingly engaging and attempting to engage monetary transactions by, through, and to a financial institution, affecting interstate and foreign commerce, in criminally derived property of a value greater than \$10,000, that is, withdrawals, deposits, purchases, and wire transfers of funds, such property having been derived from a specified unlawful activity, to wit: wire fraud, in violation of Title 18, United States Code, Section 1343, in violation of Title 18, United States Code, Section 1957.

13. Having gained control of the stolen funds as described in paragraphs 1 through 10 of this superseding indictment, the Defendants next laundered those funds through the domestic banking system and converted the funds to U.S. currency. They did so almost exclusively through the following steps:

a. *Cashier's Checks.* When a given Defendant received funds into an account he controlled, he would purchase one or more cashier's checks, funded by the fraud proceeds, and made payable to a shell company owned by a co-conspirator and created for the purpose of laundering funds. On occasion, Defendants would purchase cashier's checks, funded by fraud proceeds, and made payable to a co-conspirator in that co-conspirator's actual name.

b. *Cashing the Cashier's Checks.* Defendants would then cash the cashier's checks in exchange for U.S. currency. Most checks were cashed at the same check cashing location, New Dolton Currency Exchange in Dolton, Illinois, while some other checks were transferred to bank accounts under the Defendants' control by regular bank check. Defendants often used false identification documents as part of this process in order to make the check-casher's records appear as though an authorized person presented the check for payment.

14. Defendants executed these transactions in order to conceal the nature, source, and disposition of funds stolen from the e-mail compromise victims. The ultimate disposition of the proceeds in U.S. currency resulted in the stolen funds becoming nearly untraceable and thus unrecoverable. All of the transactions, moreover, involved more than \$10,000 in funds derived from the computer hacking scheme.

All in violation of Title 18, United States Code, Section 1956(h).



FORFEITURE SPECIFICATION

The Grand Jury further charges:

15. The allegations of Counts 1 and 2 are hereby re-alleged and incorporated herein by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Section 981(a)(1)(C), Title 18, United States Code, Section 982(a)(1), and Title 28, United States Code, Section 2461(c). As a result of the foregoing offenses, Defendants EMMANUEL OKEREKE, OLABODE BANKOLE, INDIA BARNES, OLALEKAN BASHIRU, ARUAN DRAKE, EMMANUEL ESSILFIE, JEREMIAH GLINSEY, LON GOODMAN, D'ANDRE HASTY, KINGSLEY OWUSU, ANTON PARKER, and CARLTON PRUITT shall forfeit to the United States: all property, real and personal, which constitutes, or is derived from, proceeds traceable to the violations charged in Count 1; and, all property, real and personal, involved in the violations charged in Count 2, and all property traceable to such property; including, but not limited to, the following:

a. \$763.15 seized pursuant to the execution of a federal seizure warrant on August 29, 2022, from JPMorgan Chase Bank account number x2191. The account is in the name of "Nita-Ing Sales" and is associated with BASHIRU.

b. \$529,129.85 seized pursuant to the execution of a federal seizure warrant on August 29, 2022, from JPMorgan Chase Bank Cashier's Check account number x1359. This \$529,129.85 was initially deposited into JPMorgan Chase Bank account number x2191 and, thereafter, was used to purchase the following cashier's checks:

i. JP Morgan Chase Bank Cashier's Check x2568, in the amount of \$169,670.35, dated August 15, 2022, payable to Primetime Movers Reliance LLC and associated with BASHIRU.

ii. JP Morgan Chase Bank Cashier's Check x2569, in the amount of \$189,459.50, dated August 15, 2022, payable to Multichoice Concept LLC and associated with BASHIRU.

iii. JP Morgan Chase Bank Cashier's Check x2588, in the amount of \$85,000.00, dated August 15, 2022, payable to Sparkle Transport Service Inc and associated with BASHIRU.

iv. JP Morgan Chase Bank Cashier's Check x2589, in the amount of \$85,000.00, dated August 15, 2022, payable to Primetime Movers Reliance LLC and associated with BASHIRU.

A TRUE BILL.

Original document - Signatures on file with the Clerk of Courts, pursuant to the E-Government Act of 2002.